UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/696,200	10/28/2003	David M. Chess	GB920030050US1	7325

66517 7590 12/22/2008

STEVEN E. BACH, ATTORNEY AT LAW
10 ROBERTS ROAD
NEWTOWN SQUARE, PA 19073

EXAMINER	
HOANG, DANIEL L	
ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
12/22/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/696,200	CHESS ET AL.	
	Examiner	Art Unit	
	DANIEL L. HOANG	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 September 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

RESPONSE TO ARGUMENTS

Applicant's arguments filed 9/05/08 have been fully considered but they are not persuasive. Applicant argues the following:

a) Hollander does not teach executing a hook routine in response to a system call.

b) Applicant further argues that overwriting the API does not disclose or suggest executing a hook routine at a location of the system call as a patch is not a hook routine.

c) Detection of a system call is not the same as executing a hook routine in response to a system call.

d) Hollander is silent as to how the interception component operates.

e) Hollander does not teach determining a first and a second data flow or process related to that of said call.

f) Hollander does not teach generating a consolidated information flow diagram.

In response to a), examiner respectfully disagrees. It appears applicant is arguing that the claimed "hook routine" differs from the hooking taught by Hollander. Examiner disagrees and believes the two to be analogous. If applicant contends this then applicant is required to clearly show where within the specification or the claim language the definition of a hook routine differs from that of the hooking taught by Hollander.

In response to b), examiner has not relied on patching, but rather hooking. col. 8, lines 37-44 distinguishes between hooking and patching. The hooking taught by Hollander is viewed as applicant's claimed "executing a hook routine".

In response to c), Hollander not only detects the system call but also intercepts it and redirects the API function calls to execute user-supplied custom code instead. This redirecting takes place after the system call is detected. This is viewed as being the same as executing in response to a system call.

In response to d), col. 7, lines 65-67 and col. 8, lines 1-30 describe how the interception component operates.

In response to e), examiner respectfully disagrees. First, col. 7, lines 9-14 teach a system call request. col. 7, lines 30-38 teach a list of active processes being monitored. Examiner views this to be analogous to the claimed "determining a data flow or process" and "determining another data flow or process".

In response to f), examiner respectfully disagrees. Col. 8, lines 18-30 describe the API Interception Structure Table which examiner views as analogous to the claimed "information flow diagram".

Due to the above arguments, the previous action's rejections are maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-14 are rejected under 35 U.S.C. 102(b) as being anticipated by Hollander US Patent No. 6823460.

As per claim 1, 8 and 14 Hollander teaches:

A method for detecting malicious software within or attacking a computer system, said method comprising the steps of:

in response to a system call, executing a hook routine at a location of said system call to

(a) determine a data flow or process requested by said call,

[see col. 6, lines 7-11, wherein types of system calls are detected.]

(b) determine another data flow or process for data related to that of said call,

[see col. 6, lines 12-20, wherein the types of system calls include process creation and process termination]

(c) automatically generate a consolidated information flow diagram showing said data flow or process of said call and said other data flow or process, and after steps (a-c),

[see fig. 7, wherein the API flow table is considered analogous to a "consolidated information flow diagram"]

(d) call a routine to perform said data flow or process requested by said call.

[see fig. 10, element 200]

As per claim 2, Hollander teaches:

A method as set forth in claim 1, wherein a user monitors said information flow diagram and compares the data flow or process of steps (a) and (b) with a data flow or process expected by said user.

[see col. 2, lines 45-52, "predefined rules"]

As per claim 3 and 9, Hollander teaches:

A method as set forth in claim 1, wherein said information flow diagram illustrates locations of said data at stages of a processing activity.

[see fig. 3, elements 154-165]

As per claim 4 and 10, Hollander teaches:

A method as set forth in claim 1, wherein said system call is selected from the set of: open file, copy file to memory, copy memory to register, mathematical functions, write to file, and network or communication functions.

[see col. 3, lines 64-67 and col. 4, lines 1-10]

As per claim 5 and 11, Hollander teaches:

A method as set forth in claim 1, wherein said system call is a software interrupt of an operating system.

[see col. 1, lines 65-67 and col. 2, lines 1-3, and rejection of claim 4]

As per claim 6 and 12, Hollander teaches:

A method as set forth in claim 1, wherein said system call causes a processor to stop its current activity and execute said hook routine.

[see fig. 2, element 56]

As per claim 7 and 13, Hollander teaches:

A method as set forth in claim 1 wherein said system call is made by malicious software.

[see col. 1, lines 65-67 and col. 2, lines 1-3]

As per claim 15, Hollander teaches:

A method as set forth in claim 1, wherein said hook routine is at a location pointed to by said system call.

[see col. 9, lines 12-35]

CONCLUSION

1. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

*. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulaney Street
Alexandria, VA 22314

*. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Daniel L. Hoang/

Examiner, Art Unit 2436

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436